REMARKS

Claims 1, 3-12 and 14–22 are pending in the present application. By this Amendment, claims 1, 11 and 22 have been amended. No new matter has been added. It is respectfully submitted that this Amendment is fully responsive to the Office Action dated December 2, 2005.

Drawing Objection:

The drawings are objected to under 37C.F.R. § 1.83(a), on page 2 of the Action, as not showing every feature of the invention specified in the claims.

More specifically, the Examiner contends that the "Illegal Access Discriminating Apparatus" is not shown in the drawings. However, it is respectfully submitted that the Examiner's position is clearly incorrect, since, for example, the illegal access discriminating system 16 is clearly illustrated in Figs. 1 and 7. Accordingly, withdrawal of the objection to the drawings is respectfully requested.

Claim Objection:

Claim 1 is objected to on page 3 of the action due to the misspelling of the word "information." It is respectfully submitted that claim 1 has been amended to correct this typographical error. Accordingly, withdrawal of this objection is respectfully requested.

Claim Rejections 11 and 22 - 35 U.S.C. § 112

Claims 11 and 22 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

This rejection is respectfully traversed.

It is respectfully submitted that claims 11 and 22 have been amended to overcome this rejection. Accordingly, withdrawal of this rejection is respectfully requested.

As To The Merits:

As to the merits of this case, the Examiner sets forth the following rejections:

1) claims 1, 5 and 12 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Moussa et al. (USP 6,035,406) in view of McNair (USP 5,276,444); and

2) claims 3, 4, 6-11, 12 and 14-22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Moussa et al. (USP 6,035,406), and further in view of McNair (USP 5,276,444) and Gressel (USP 6,311,272).

Each of these rejections is respectfully traversed.

At the outset, it is respectfully submitted that the illegal access discriminating apparatus of the present invention is different from an authentication apparatus in a service providing system as shown in the attached drawing.

The present invention does not provide a response to a request for a personal authentication by accessing a service providing system. In general, a service providing system has a configuration of giving an authentication for authorization to use to a user by registering user's ID and biometrics information in advance, and collating with these registered pieces of information. The present invention relates in contrast to an illegal access discriminating apparatus which detects an illegal access to a service providing apparatus. It detects an illegal access in a prior stage to the biometrics authentication (user ID+ biometrics) of a usual service providing system.

The attached drawing shows the features of the present invention as "Range of implementation of the present invention" in a box.

<Implementation range of the present invention relative to the conventional biometrics authentication system>

Independent Claims 1 and 12:

Independent claim 1 calls for *a second storing unit for storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time,*

wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication. Independent claim 12 includes similar features.

In addition, claim 1 calls for *a comparing and collating unit for comparing and collating the latest inputted ID information and organic information with all of ID information and organic information stored in said second storing unit which were inputted and not previously registered in the past.* Again, independent claim 12 includes similar features.

The Examiner rejects the present invention by citing Moussa, col. 3, lines 24-33 and col. 5, lines 56-64. However, Moussa's document has no relevance to the present invention. The cited portions of Moussa give expression such as "an authentication fingerprint F' and "the data block fingerprint D with the fingerprint F it has stored in the authentical database". However, the term "fingerprint" referred to in the present invention concerns a human fingerprint ("origin information" recited in. claim 1 of the present invention). The fingerprint in the cited reference means a hash value[1] (*1) of a certain data, as described in col.4, lines 50-54.

[1] In the encryption sector of industry, a hash value used in an electronic signature or the like is often called a "fingerprint". For example, when performing an "https" communication upon entering a password in Internet Explorer, a key mark appears in the right bottom of the screen. If this is clicked, you will understand that a bash value in an open certificate used cryptographic communication is displayed by an expression "fingerprint". Popularly used hash values include "MD5 fingerprint" and "SHA1 fingerprint".

This fact is evident from Moussa's document, col. 6, lines 64-67. This portion of Moussa gives a description, "The login service 140 generates a new fingerprint F* in response to the new data block 132, in like manner as the data block fingerprint D is computed in the sub-step 224(b)." This expresses that a new "fingerprint" is prepared from a data block 132. This means that a new fingerprint (hash value) is created from data written in the data block 132. It is not correct to interpret this fingerprint as being a human fingerprint which is invariable all the life.

Moussa's document cannot therefore be an example of a publicly known document of the present invention.

As such, it is submitted that Moussa fails to disclose or fairly suggest the features of claim 1 concerning *a second storing unit for storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time, wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication; a comparing and collating unit for comparing and collating the latest inputted ID information and organic information with all of ID information and organic information stored in said second storing unit which were inputted and not previously registered in the past.*

Moreover, it is submitted that the secondary references of McNair and Gressel each fail to teach or fairly suggest these above-noted drawbacks and deficiencies of the primary reference of Moussa.

Further, the Examiner correctly acknowledges (in the bridging sentence between pages 4 and 5 of the Action) that the primary reference of Moussa also fails to disclose the features of claim 1 concerning *a control unit for discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy predetermined conditions and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value.*

In order to compensate for these deficiencies of Moussa, the Examiner relies on the secondary reference of McNair and contends that McNair "teaches a threshold per biometric sample type that can possibly be used by each individual in order to indicate an attacker in the event of numerous unsuccessful authentication attempts," (see, lines 1-3, page 5 of the Action).

However, it is respectfully submitted that while McNair may be concerned with a "try again" threshold, in which access is denied but the requester may be allowed to supply a different form of authentication information to obtain access, McNair is completely silent with regard to *discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy predetermined conditions and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value,* as called for in claim 1.

Further, with regard to Gressel, the Examiner describes only the setting of such reference. Gressel says only that in an environment under supervision by a security camera or the like, it

suffices to ensure a threshold value of a personal refusal rate of about once per 500, i.e., an FAR threshold of 100 is reasonable. This is followed by the cited portion (col. 10, Lines 35-39) which states only that a looser threshold of 200 will do in a placed of a higher frequency of use such as an amusement park, and contains no expression relating to the present invention.

As such, in view of the above, it is respectfully submitted that neither Moussa, McNair, nor Gressel, singly or in combination, disclose or fairly suggest the features of claim 1 concerning *a second storing unit for storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time, wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication; a comparing and collating unit for comparing and collating the latest inputted ID information and organic information with all of ID information and organic information stored in said second storing unit which were inputted and not previously registered in the past; and a control unit for discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy predetermined conditions and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value.*

Claim Rejections 3 and 14 - 35 U.S.C. § 103(a)

The Examiner contends that Moussa, when viewed with McNair and Gressel, discloses what is presently taught in claim 3. The Examiner states the Moussa and McNair do not disclose:

> "a control unit [that] determines that there is the authentication demand by the illegal access person in the case where the ID information does not coincide and the organic information coincides or the case where the ID information coincides and the organic information does not coincide on the basis of the output of said comparing and collating unit."

The Examiner however, asserts that Gressel "teaches two typical proximity thresholds for biometric sampling, which are monitored for imposters attempting to enter unauthorized," (col. 10, lines 26-34), and that "3% of the population would be rejected regardless of the value of the threshold" and that "human intervention then becomes necessary to process the applicant," (col. 10, lines 48-54).

Lines 26-34 of Gressel explain figure 9A, which is a graph describing the False Rejection Rate (FRR) and False Acceptance Rate (FAR) of a "Digi-2 finger geometry identification device.[2]" As would be predicted by one ordinarily skilled in the art, false rejections increase as the verification threshold criteria tightens, and false acceptances decrease. As expected, the opposite results are attained if the verification threshold criteria are loosened.

It is respectfully submitted that the passages in Gressel, cited by the Examiner, do not disclose what is taught in claims 3 (recited above), and 14, and have little if any relevance to the present invention.

[2] As disclosed in Gressel, a "Digi-2 finger geometry identification device" is an electro-optical fingerprint reader, which is publicly available.

Claim Rejections 4 and 15 - 35 U.S.C. § 103(a)

The Examiner contends that when Moussa is viewed in light of McNair and Gressel, it would have been obvious to one ordinarily skilled in the art to combine the three, and that therefore, claims 4 and 15 were previously disclosed. Claim 4 involves:

> said control unit determines that there is the authentication demand by the illegal access person in the case where the comparison result by said comparing and collating unity between the inputted ID information and the past ID information inputted from a same terminal position within a predetermined time indicates dissidence.

In other words, the present invention is able to factor in; the difference in time between two possible illegal access attempts, and whether or not the same terminal was used, in order to help determine if an illegal access was being attempted.

Gressel discloses that "upon successful completion of the bio-test, the user's biometric features are encoded into the smart card," (column 12, lines 42-43). The Examiner contends that "it would have been obvious to combine Gressel's teachings to Moussa and McNair, because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins."

It appears that the Examiner is arguing that the amount of time between inputting two different identification methods (such as performing a bio-test and encoding a smartcard), during the same overall access attempt, is the same as the amount of time between two different and distinct access attempts. Claims 4 and 15 teach discerning an illegal access attempt using the

latter method, while it is asserted by the Examiner that Gressel implies the former method. As is apparent on its face, the two methods are not the same.

For at least these reasons, Moussa, McNair, and Gressel, when viewed singly or in any combination, do not disclose or fairly suggest the elements of claims 4 or 15.

In view of the aforementioned amendments and accompanying remarks, Applicants submit that that the claims, as herein amended, are in condition for allowance. Applicants request such action at an early date.

If the Examiner believes that this application is not now in condition for allowance, the Examiner is requested to contact Applicants' undersigned attorney to arrange for an interview to expedite the disposition of this case.

If this paper is not timely filed, Applicants respectfully petition for an appropriate extension of time. The fees for such an extension or any other fees that may be due with respect to this paper may be charged to Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP

Thomas E. Brown
Attorney for Applicants
Registration No. 44,450
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

TEB/jl

Attachment: Drawing showing implemented range of the present invention relative to the conventional biometrics authentication system.